UNITED STATES DISTRICT COURT

for the

Eastern District of Pennsylvania

In the Matter of the Search of
(Briefly describe the property to be searched or identify the person by name and address)
black ZTE smartphone cellular telephone

Case No. 18-1884-M

APPLICATION FOR A SEARCH WARRANT

I, a federal law enforcement officer or an attorney for the government, request a search warrant and state under penalty of perjury that I have reason to believe that on the following person or property *(identify the person or describe the property to be searched and give its location):*
See Attachment A

located in the Eastern District of Pennsylvania, there is now concealed *(identify the person or describe the property to be seized)*:
See Attachment B

The basis for the search under Fed. R. Crim. P. 41(c) is *(check one or more)*:

- ☑ evidence of a crime;
- ☐ contraband, fruits of crime, or other items illegally possessed;
- ☑ property designed for use, intended for use, or used in committing a crime;
- ☐ a person to be arrested or a person who is unlawfully restrained.

The search is related to a violation of:

Code Section	*Offense Description*
21 U.S.C. sec. 846; 21 U.S.C. sec. 841(a)(1); 21 U.S.C. sec. 843	Conspiracy to distribute a controlled substance, distribution of a controlled substance, use of a communication facility to engage in distribution of a controlled substance

The application is based on these facts:
See Affidavit

- ☑ Continued on the attached sheet.
- ☐ Delayed notice of _____ days (give exact ending date if more than 30 days: _____) is requested under 18 U.S.C. § 3103a, the basis of which is set forth on the attached sheet.

Applicant's signature

William J. Becker IV, Special Agent, FBI
Printed name and title

Sworn to before me and signed in my presence.

Date: 11/20/18

Judge's signature

City and state: Philadelphia, Pennsylvania

Honorable Elizabeth T. Hey, US Magistrate Judge
Printed name and title

AFFIDAVIT

I, William J. Becker IV, Special Agent with the Federal Bureau of Investigation ("FBI"), United States Department of Justice, being duly sworn do hereby depose and state as follows:

INTRODUCTION

1. I am an "investigative or law enforcement officer" within the meaning of Title 18, United States Code, Section 2501(7), that is, an officer of the United States who is empowered by law to conduct investigations of and to make arrests for offenses enumerated in Title 18, United States Code, Section 2516.

2. I am a Special Agent ("SA") with the Federal Bureau of Investigation ("FBI"), Philadelphia Field Division and have been employed by the FBI since March 2017. I have received specialized training from the FBI, including training in the investigation and identification of narcotics traffickers and violent gangs. During my tenure with the FBI, I have been assigned to the High Intensity Drug Trafficking Area ("HIDTA")/Safe Streets Violent Drug Gang Task Force ("SSVDGTF") of the Philadelphia Division, which investigates, among other violations of federal law, violent drug gangs and criminal organizations including those involved in the importation, distribution and manufacturing of controlled substances, Hobbs Act violations, outlaw motorcycle gangs, and homicides and shootings resulting from the drug trade. Prior to my employment with the FBI, I served as a Police Officer with the Whitpain Township Police Department, Montgomery County, Pennsylvania from September 2010 until March 2017. During my tenure with the Whitpain Township Police Department, I received specialized training in narcotics enforcement, and served as a Task Force Officer with the Montgomery County Drug Task Force. While a police officer and an agent, I have investigated numerous firearms violations, drug violations, and other related crimes. I have conducted physical and

electronic surveillance, debriefed confidential sources, analyzed information obtained from court-authorized pen register and trap and trace intercepts, and participated in the drafting and execution of search warrants involving these matters. I am an active investigator for the FBI Gangs and Criminal Enterprise Program in which state and local arrests for drugs and firearms violations are reviewed and referred for possible federal prosecution. I have specialized training and experience in drug smuggling and distribution investigations, including but not limited to, the means and methods used by traffickers to import and distribute drugs, interdiction, smuggling methods, and the concealment and laundering of proceeds from illicit drug trafficking activities.

3. I have participated in numerous narcotics investigations, debriefed or participated in debriefings of numerous of defendants, informants and witnesses who had personal knowledge regarding major drug trafficking organizations, and have participated in all aspects of drug investigations. I have participated in all aspects of narcotics investigations including surveillance, analyzing information obtained from court-authorized pen register and trap and trace intercepts, Title-III wiretap investigations, and analyzing telephone toll records. I am aware that drug traffickers commonly use cellular telephones and other electronic devices in furtherance of their drug trafficking activities and frequently change cellular telephone numbers and cellular phones in an effort to thwart law enforcement's use of electronic surveillance.

4. Through my training and experience and the training and experience of the law enforcement officers involved in this investigation, your affiant is aware that drug traffickers often use cellular phones, through phone calls, text messages, voice messages and emails, to arrange for the purchase of illegal narcotics. I am aware that cellular telephones are all

identifiable by unique numbers on each phone, including: serial numbers, international mobile equipment identification (IMEI) numbers, and/or electronic serial numbers (ESN). I know that drug traffickers commonly maintain in their cellular phones, the contact information of co-conspirators, sources of supply, and customers, such as names or nicknames, phone numbers, pager numbers, addresses and other identifying information. Additionally, I know that drug traffickers use cell phones to take pictures of themselves and co-conspirators with drugs, weapons, cash and drug paraphernalia.

6. I make this affidavit in support of an application for a search warrant of a black ZTE cellular phone, recovered during the arrest of DENNIS HARMON that took place on September, 11 2017 by Philadelphia Police. The black ZTE cellular telephone is hereafter referred to as the "TARGET TELEPHONE" which is listed in Attachment A. This application seeks authority to search for and seize evidence, and fruits and instrumentalities of crimes against the United States, specifically in violation of Title 21, United States Code, Sections 846, 843(b) and 841(a)(1), as described in Attachment B.

7. The probable cause set forth in this affidavit is based upon my personal knowledge, information provided by a confidential human source (CHS), surveillance conducted by law enforcement officers involved in this investigation, and the experience and training of law enforcement officers. Because this affidavit is being submitted for the limited purpose of establishing probable cause for the search of the TARGET TELEPHONE, I have not set forth each and every fact learned during the course of this investigation, but only those facts necessary to establish such probable cause.

BACKGROUND OF INVESTIGATION

1. This application is submitted in support of a FBI investigation into a drug violent trafficking organization, believed to operate primarily in Philadelphia with connections in California, Las Vegas, and various parts of the United States, including the Eastern District of Pennsylvania. The United States, including the FBI, is conducting a criminal investigation of the drug trafficking organization regarding possible violations of Title 21, United States Code, Sections 846, 841(a)(1).

2. Since March 2017, the FBI and the Philadelphia Police Department have been investigating a violent drug trafficking organization known as the Original Block Hustlaz (OBH) gang and several targets that are believed to be members of the organization, including Abdul WEST, the leader of the OBH gang. The OBH gang is involved in drug trafficking and violence primarily in the Philadelphia area. Agents and officers have conducted numerous controlled narcotics purchase operations from OBH members or subjects believed to be supplied by OBH members and associates as well as conducted numerous surveillance operations of suspected narcotics transactions. OBH gang members also have a large social media presence which is monitored by the FBI. Much of the social media activity of the gang members discusses or suggests the ongoing illegal activities of the gang. Additionally, the Philadelphia FBI and the Philadelphia Police Homicide unit are currently investigating three homicides and three non-fatal shootings that are directly related to or carried out by members of the OBH gang. Specifically, investigators have evidence to believe that one of those homicides was carried out by an OBH gang member or associate as part of a drug robbery. Drugs from that robbery were later sold to an FBI confidential informant and are currently evidence in the custody of the FBI.

3. As stated in paragraph #2, investigators have conducted numerous controlled narcotics and a firearm purchase from OBH gang members. Confidential Informants and undercover Law Enforcement Officers utilized cellular telephones to communicate with members of OBH to arrange and execute these controlled purchase operations.

4. On September 11, 2017, Philadelphia Police Officers conducted a search warrant in furtherance of a homicide investigation of the address 3234 North Sydenham Street, Philadelphia, PA, which members of OBH and their associates refer to as "the Mansion." Inside the residence officers seized approximately 240 grams of heroin, 65 grams of crack cocaine, 52 grams of methamphetamine, and 1200 grams of marijuana. They also located and seized $8,101.00 in United States Currency and a .45 caliber handgun. Shortly before Police Officers arrived to secure the residence for the search, FBI surveillance observed, via a pole camera, ABDUL WEST, DENNIS HARMON, and other individuals known to be OBH members coming and going from the residence. Upon the arrival of Police Officers, all of the males congregating around the residence left the area, including WEST and HARMON. HARMON then returned to the residence not long thereafter, and was questioned by Philadelphia Police Officers. HARMON advised the Officers that he was the only person at the residence and that he was squatting there. HARMON was also observed, via the pole camera, utilizing a cellular telephone; this cellular telephone was seized by the Philadelphia Police Department and was determined to be the TARGET TELEPHONE, identified on Philadelphia Police property receipt number 3382320. HARMON was then taken into custody and subsequently charged by the Philadelphia Police Department with Possession with Intent to Deliver (a controlled substance), as well as additional misdemeanor controlled substance charges.

5. On October 17, 2018, DENNIS HARMON and ABDUL WEST were charged in a Superseding Indictment with violating the following statute: possession with intent to distribute 28 grams or more of a mixture and substance containing a detectable amount of cocaine base ("crack"), 100 grams or more of a mixture and substance containing a detectable amount of heroin, and approximately 48 grams of a mixture and substance containing a detectable amount of methamphetamine.

6. During the course of this investigation, law enforcement has executed search warrants on the phones of co-defendants in this case which have contained evidence of narcotics trafficking, including communications regarding police activity at "the Mansion" (3234 Sydenham Street), meetings to exchange drugs and drug proceeds, coordinating deliveries of narcotics, and protection of stash houses where drugs and drug proceeds are kept.

7. Based on training and experience, your affiant believes that important data recovered from the TARGET TELEPHONE, including the call logs, phone books, contacts lists, and text messages, will provide valuable information that will further the investigation of the drug trafficking organization.

8. Based on my training and experience, I know that individuals involved in drug trafficking often maintain more than one phone or more than one SIM card device, in order to have multiple avenues to facilitate drug trafficking activities, and in an attempt to avoid detection by law enforcement. I am aware that individuals involved in drug trafficking often times utilize pre-paid cellular telephones which do not maintain specific subscriber information, and/or use phones subscribed to in the name of third person, in order to mask their direct linkage to telephones utilized in furtherance of drug trafficking activities. Further, those involved in drug

trafficking often change SIM cards in order to make it difficult for law enforcement to determine their records. Based on my training and experience, I know that individuals involved in drug trafficking also frequently switch telephone numbers and/or phones. Despite the constant switching of active telephone numbers, drug traffickers often keep old phones.

9. Based on my training and experience, I know that drug traffickers commonly utilize their cellular telephones to communicate with co-conspirators to facilitate, plan, and execute their drug transactions. For example, I know that drug traffickers often store contacts lists, address books, calendars, photographs, videos, and audio files, text messages, call logs, and voice mails in their electronic devices, such as cellular telephones, to be used in furtherance of their drug trafficking activities.

10. Based on my training and experience, I know that information stored on cellular telephones can often be retrieved months or even years later using forensic tools.

11. Specifically, I know that those involved in drug trafficking communicate with associates using cellular telephones to make telephone calls. If they are unable to reach the party called, they frequently leave voice mail messages. I am aware that Apple-based and Android-based phones download voice mail messages and store them on the phone itself so that there is no need for the user to call in to a number at a remote location and listen to the message. In addition, I know those involved in drug trafficking communicate with associates using cellular telephones and tablets to send e-mails and text messages and communicate via social media networking sites. By analyzing call and text communications, I may be able to determine the identity of co-conspirators and associated telephone numbers, as well as if there were communications between associates during the commission of the crimes.

12. Furthermore, cellular telephones also contain address books with names, addresses, photographs, and phone numbers of a person's regular contacts. I am aware that drug traffickers frequently list drug associates in directories, often by nickname, to avoid detection by others. Such directories as the ones likely contained in the seized cellular telephones, are one of the few ways to verify the numbers (*i.e.*, telephones, pagers, etc.) being used by specific traffickers.

13. In addition, I know that those involved with drug trafficking often take photographs or make videos of themselves and their co-conspirators and retain them on their electronic devices such as cellular telephones. This evidence would show associations between accomplices, *i.e.* photographs of accomplices and/or individuals common to co-conspirators. I am also aware that drug traffickers often take photographs or make videos of drugs, drug proceeds and firearms with their cellular telephones and tablets. Based on my training and experience, those who commit these crimes often store these items on their phones in order to show to associates, and/or to upload to social media.

14. Furthermore, based on my training and experience and the training and experience of other agents, I know that drug traffickers often use a cellular phone's Internet browser for web browsing activity related to their drug trafficking activities. Specifically, drug traffickers may use an Internet search engine to explore where banks or mail delivery services are located, or may use the Internet to make reservations for drug-related travel. In addition, I know that drug traffickers also use their cellular telephone's Internet browser to update their social networking sites in order to communicate with co-conspirators, and to display drugs and drug proceeds or to

post photographs of locations where they have traveled in furtherance of their drug trafficking activities.

15. In addition, drug traffickers sometimes use cellular telephones as navigation devices, obtaining maps and directions to various locations in furtherance of their drug trafficking activities. These electronic devices may also contain GPS navigation capabilities and related stored information that could identify where these devices were located.

16. Furthermore, based on my training and experience, forensic evidence recovered from the review of a cellular telephone can also assist in establishing the identity of the user of the device, how the device was used, the purpose of its use, and when it was used. In particular, I am aware that cellular telephones are all identifiable by unique numbers on each phone, including: serial numbers, international mobile equipment identification numbers (IMEI) and/or electronic serial numbers (ESN). The search of each phone helps determine the telephone number assigned to each device, thus facilitating the identification of the phone as being used by members of the conspiracy. In addition, I am aware that by using forensic tools, information/data that users have deleted may still be able to be recovered from the device.

17. Nature of examination. Based on the foregoing, and consistent with Rule 41(e)(2)(B), the warrant I am applying for would permit the examination of the TARGET TELEPHONE consistent with the warrant. The examination may require authorities to employ techniques, including but not limited to computer-assisted scans of the entire medium, that might expose many parts of the device to human inspection in order to determine whether it is evidence described by the warrant.

ELECTRONIC DEVICES

18. As described above and in Attachment B, this application seeks permission to search and seize things that the TARGET TELEPHONE might contain, in whatever form they are stored. As used herein, the term "electronic device" includes any electronic system or device capable of storing or processing data in digital form, in this case referring specifically to wireless or cellular telephones.

19. Based on my knowledge, training, and experience, as well as information related to me by others involved in the forensic examination of digital devices, I know that data in digital form can be stored on a variety of digital devices. In particular, I know that electronic devices, including cellular telephones used by drug traffickers, are likely to be repositories of evidence of crimes. I know that an electronic device such as a cellular telephone may contain data that is evidence of how the electronic device was used, data that was sent and received, and other records that may indicate the nature of the offense.

20. Furthermore, I know that electronic devices, such as cellular telephones, can store information for long periods of time. Examples of such information include text and multimedia message conversations, call history, voice mail messages, e-mails, photographs, and other data stored on the device. Similarly, I know from my training and experience that when cellular telephones are used to access the internet, a browser history is also frequently stored for some period of time on the electronic device. This information can sometimes be recovered with forensic tools.

21. Based on my experience and training, as well as the experience and training of other agents, I know that even when a user deletes information from a device, it can sometimes be recovered with forensics tools.

22. Based on my knowledge, training, and experience, as well as information related to me by agents and others involved in the forensic examination of digital devices, I know that searching electronic devices can be a highly technical process that requires specific expertise and specialized equipment. There are so many types of electronic devices and software programs in use today that specialized equipment is sometimes necessary to conduct a thorough search. In addition, it may be necessary to consult with specially trained personnel who have specific expertise in the types of electronic devices, operating systems, or software applications that are being searched.

23. I am also aware that electronic files or remnants of such files can be recovered months or even years after they have been downloaded onto a hard drive, deleted, or viewed via the Internet. Electronic files saved to a hard drive can be stored for years with little or no cost. Even when such files have been deleted, they can be recovered months or years later using readily-available forensics tools. Normally, when a person deletes a file on an electronic device, the data contained in the file does not actually disappear; rather, that data remains until it is overwritten by new data. Therefore, deleted files, or remnants of deleted files, may reside in free space or slack space, i.e., space on a hard drive that is not allocated to an active file or that is unused after a file has been allocated to a set block of storage space, for long periods of time before they are overwritten. In addition, a computer's operating system may also keep a record of deleted data in a swap or recovery file. Similarly, files that have been viewed on the Internet

are often automatically downloaded into a temporary directory or cache. The browser typically maintains a fixed amount of hard drive space devoted to these files, and the files are only overwritten as they are replaced with more recently downloaded or viewed content. Thus, the ability to retrieve residue of an electronic file from a hard drive depends less on when the file was downloaded or viewed than on a particular user's operating system, storage capacity, and computer habits. Recovery of residue of electronic files from a hard drive requires specialized tools and a controlled laboratory environment. Recovery also can require substantial time.

24. Although some of the records called for by this warrant might be found in the form of user-generated documents (such as word processing, picture, and movie files), electronic devices can contain other forms of electronic evidence as well. In particular, records of how an electronic device has been used, what it has been used for, who has used it, and who has been responsible for creating or maintaining records, documents, programs, applications and materials contained on the electronic devices are, as described further in the attachments, called for by this warrant. Those records will not always be found in digital data that is neatly segregable from the hard drive image as a whole. Digital data on the hard drive not currently associated with any file can provide evidence of a file that was once on the hard drive but has since been deleted or edited, or of a deleted portion of a file (such as a paragraph that has been deleted from a word processing file). Virtual memory paging systems can leave digital data on the hard drive that show what tasks and processes on the computer were recently used. Web browsers, e-mail programs, and chat programs often store configuration data on the hard drive that can reveal information such as online nicknames and passwords. Operating systems can record additional data, such as the attachment of peripherals, the attachment of USB flash storage devices, and the

times the electronic device was in use. Computer file systems can record data about the dates files were created and the sequence in which they were created. This data can be evidence of a crime, indicate the identity of the user of the digital device, or point toward the existence of evidence in other locations. Recovery of this data requires specialized tools and a controlled laboratory environment, and also can require substantial time.

25. Further, evidence of how an electronic device has been used, what it has been used for, and who has used it, may be the absence of particular data on an electronic device. For example, to rebut a claim that the owner of an electronic device was not responsible for a particular use because the device was being controlled remotely by malicious software, it may be necessary to show that malicious software that allows someone else to control the electronic device remotely is not present on the electronic device. Evidence of the absence of particular data on an electronic device is not segregable from the electronic device. Analysis of the electronic device as a whole to demonstrate the absence of particular data can require specialized tools and a controlled laboratory environment, and can require substantial time.

26. Searching for the evidence described in Attachment B may require a range of data analysis techniques. In some cases, law enforcement officers and computer analysts may be able to conduct carefully targeted searches that can locate evidence without requiring a time consuming manual search through unrelated materials that may be co-mingled with criminal evidence. In other cases, however, such techniques may not yield the evidence described in the warrant. Criminals can mislabel or hide information, encode communications to avoid using key words, attempt to delete information to evade detection, or take other steps designed to frustrate law enforcement searches for information. These steps may require agents and law enforcement

or other analysts with appropriate expertise to conduct more extensive searches, such as scanning storage areas unrelated to things described in Attachment B, or perusing all stored information briefly to determine whether it falls within the scope of the warrant. In light of these difficulties, law enforcement intends to use whatever data analysis techniques appear necessary to locate and retrieve the evidence described in Attachment B.

SUMMARY AND CONCLUSION

27. Based on the foregoing facts, your affiant believes that there is probable cause that the fruits and/or evidence of crimes specifically, violations of Title 21, United States Code, Sections 846, 843 and 841, as enumerated in Attachment B, will be found in the information stored in the TARGET TELEPHONE. This phone has remained in the custody of the Philadelphia Police Department, in the Eastern District of Pennsylvania, since being recovered on or about September 11, 2017, and was transferred to the custody of FBI Philadelphia on November 2, 2018. Accordingly, I respectfully request that the Court issue a warrant to search the TARGET TELEPHONE. Because this search will not involve any intrusion on any physical location and seeks to search a telephone already in law enforcement custody, your affiant requests permission to conduct the search of the TARGET TELEPHONE at any time of the day or night.

Your affiant declares under penalty of perjury that the foregoing is true and correct to the best of his knowledge and belief, and that this declaration was executed on:

William J. Becker IV, Special Agent
Federal Bureau of Investigation

Sworn and subscribed before me
this 20th day of November, 2018.

HONORABLE ELIZABETH T. HEY
United States Magistrate Judge

ATTACHMENT A: "TARGET TELEPHONE" TO BE SEARCHED

A black ZTE smartphone, currently in the custody of the Federal Bureau of Investigation, Philadelphia, PA.

ATTACHMENT B

ITEMS TO BE SEIZED

The telephones listed in Attachment A may be searched for evidence of the following violations: conspiracy to distribute a controlled substance in violation of Title 21, United States Code, Section 846; distribution, and possession with intent to distribute, a controlled substance in violation of Title 21, United States Code, Section 841(a)(1); and use of communication facilities to facilitate narcotics trafficking offenses in violation of Title 21, United States Code, Section 843, including:

a. Electronic communications relating to the criminal activity,

b. Telephone or address directory entries consisting of names, addresses, telephone numbers; logs of telephone numbers dialed, telephone numbers of incoming, outgoing or missed calls, text messages, schedule entries, stored memoranda, videos, social networking sites and digital photographs,

c. Lists of customers and related identifying information,

d. Types, amounts, and prices of drugs trafficked as well as dates, places, and amounts of specific transactions,

e. Any information related to sources of controlled substances, including names, addresses phone numbers, and any other identifying information,

f. Any information related to the methods of trafficking in controlled substances,

g. Any information recording domestic and international schedule or travel related to the described criminal activity, including any information recording a nexus to airport facilities, airport security, or airlines,

h. All bank records, checks, credit cards, credit card bills, account information, and other financial records,

i. All data that has been manually programmed into a GPS navigation system, as well as data automatically stored by the GPS navigation system,

j. Stored memoranda; stored text messages, including drafts; stored voicemail messages; stored electronic mail; stored photographs; stored audio; and stored video,

k. Evidence of the presence or absence of software that would allow others to control the device, such as viruses, Trojan horses, and other forms of malicious software, as well as evidence of the presence or absence of security software designed to detect malicious software,

l. Evidence of the attachment of other devices,

m. Evidence of counter-forensic programs (and associated data) that are designed to eliminate data from the device,

n. Evidence of the times the device was used,

o. Passwords, encryption keys, and other access devices that may be necessary to access any of the devices,

p. Records of or information about Internet Protocol addresses used by the device,

q. Records of or information about the device's Internet activity, including firewall logs, caches, browser history and cookies, "bookmarked" or "Favorite" web pages, search terms that the user entered into any Internet search engine, and records or user-typed web addresses, as well as evidence of the posting of videos, photos, or any material relevant to these crimes to any social networking site.

r. Evidence of user attribution showing who used or owned the electronic devices at the time the things described above were created, edited, or deleted, such as logs phonebooks, saved usernames and passwords, documents, and browsing history;

s. any other information pertaining to the possession, receipt, and/or distribution of narcotics that were transmitted, stored, or received using the item to be searched.